



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET

WASHINGTON, D.C. 20503

May 7, 1976

OMB Declassification/Release Instructions on File

LEGISLATIVE REFERRAL MEMORANDUM

*OMB Advised
No Comment
5/11/76
PLC
Legislation*

TO: Legislative Liaison Officer
National Security Council
Department of State
Central Intelligence Agency
Department of Justice

SUBJECT: DOD's proposed statement re H.R. 169 and H.R. 12039,
"To amend the Privacy Act of 1974"

The Office of Management and Budget requests the views of your agency on the above subject before advising on its relationship to the program of the President, in accordance with OMB Circular A-19.

A response to this request for your views is needed no later than Monday, May 10, 1976.

Questions should be referred to Robert Carlstrom (395-3856) or to-----the legislative analyst in this office.

Bernard H. Martin

Bernard H. Martin for
Assistant Director for
Legislative Reference

Enclosures

bc

TESTIMONY OF
DAVID O. COOKE
DEPUTY ASSISTANT SECRETARY OF DEFENSE
(ADMINISTRATION)
BEFORE THE
GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS SUBCOMMITTEE
OF THE COMMITTEE ON GOVERNMENT OPERATIONS
HOUSE OF REPRESENTATIVES,
ON
H.R. 169 and H.R. 12039
TO AMEND THE PRIVACY ACT OF 1974

May 11, 1976

Madam Chairwoman, Members of the Subcommittee:

I appreciate the opportunity to appear before you today to present the views of the Department of Defense on H.R. 169 and H.R. 12039. Inasmuch as the provisions of H.R. 169 have been included in the more comprehensive provisions of H.R. 12039, my remarks will address the latter bill.

H.R. 12039 consists of five amendments to the Privacy Act of 1974. Of the five amendments, amendments (4) and (5) relate solely to the operations of the Central Intelligence Agency and the Secret Service. Consequently, the Department of Defense will confine its comments to amendments (1) and (2). We are concerned with amendment (3) only because it precludes a law enforcement agency from taking an exemption to Amendment 2.

Amendment (1) would permit the individual to request the Agency to correct his record if the individual believes that the record is not "legally maintained." Should the Agency determine that the record is not legally maintained, or if the record is not accurate, relevant, timely or complete, the Agency may correct the record, or expunge, update or supplement any parts thereof. As this amendment merely adds explanatory language to the procedures for correcting records, the Department of Defense has no objections.

Amendment (2) would require that certain classes of individuals be notified by the Agency of their rights under the Freedom of Information and Privacy Acts. It would further give that person the "option of requiring that Agency to destroy such copies of each file or index in its possession." The following categories of persons would be entitled to notification, and, at their election, to destruction of their records:

(A) Any sender or receiver of a communication which was intercepted or examined by the Agency without a search warrant, or without the consent of both parties.

(B) Any occupant, resident or owner of any premises or vehicle which is searched by the Agency without a search warrant, or without the consent of such person.

(C) Any person who is the subject of a file or named in an index maintained in connection with Operation CHAOS, COINTELPRO, or "The Special Service Staff."

As Category (C) above, Operations CHAOS, COINTELPRO and "The Special Service Staff," relates to the Central Intelligence Agency, the Federal Bureau of Investigation and the Internal Revenue Service, the Department of Defense defers to the comments of those agencies. However, the Department has noted that the decision of the Attorney General to notify persons who were subjects of the Operation COINTELPRO is dependent upon a showing that the specific COINTELPRO activity was improper, that actual harm may have occurred and that

the subjects were not already aware that they were the targets of such activity.

As for including the categories of persons described in (A) and (B) above, the Department of Defense is opposed to amendment (2) for a number of reasons:

The kinds of records maintained by the Department of Defense under categories (A) and (B) above are clearly distinguishable from the kind of activities which had been directed against certain individuals by the Federal Bureau of Investigation, the Central Intelligence Agency and the Internal Revenue Service. In the course of carrying out investigations, the Department may engage in the interception of communications at the request of one of the parties but not both parties. Under such circumstances, this interception is not a violation of law and is not a basis for civil action for damages. Chapter 119 of Title 18 U.S.C. expressly provides that it shall not be unlawful to intercept a wire or oral communication where "one of the parties to the communication has given prior consent to such interception." U.S. v. Rich, 1975, 518 F.2d 980. Bakes v. U.S. 350 F. Supp. 547, affirmed 748 F. 2(b) 1405. Moreover, consensual interceptions have been ruled as not violating the accused rights of privacy under the Fourth Amendment. See Com. v. Donnelly, Pa. Super. 1975, 336 A. 2d 632. Consequently, no harm has occurred and there is no basis for providing the unconsenting party with the option of requiring the destruction of the records.

Amendment (2) also fails to take into account that not all searches of premises or vehicles without a search warrant or the consent of the resident or owner are illegal. For example, the Commanding Officer of a military unit may authorize, on probable cause, a search of the property of a person subject to military law or a search of military property. Within the civilian community, law enforcement officers are entitled under certain circumstances to the search of premises or vehicles without a search warrant, when the search is for instrumentalities or fruits of the crime, property the possession of which is itself a crime, or evidence which there is reason to believe will otherwise aid in a particular apprehension or conviction. Again, these searches, and the records of such searches, are clearly distinguishable from the particular tactics that were directed at individuals or organizations under COINTELPRO.

The notification requirement would adversely affect the ability of law enforcement agencies to intercept criminal conversations where one party has given his consent. Of course, if neither party consents the Department would be required to obtain a warrant as required by Chapter 119 of Title 18 U.S.C. For example, consensual eavesdrops are used in narcotics related offenses in which a consenting source of information voluntarily allows interception of communications between himself and suspected drug dealers. The interception of these conversations serves not only to provide documentary evidence in subsequent court proceedings, but also serves

as a means of protecting the sources during his contact with potentially hostile subjects. But, under the terms of H.R. 12039, suspected drug dealers could not only determine the identity of the source who contributed the information, but demand the destruction of the evidence gathered by the intercept.

There are other areas of law enforcement in which the notification and destruction provisions would also significantly hamper what are now successful and legal techniques. For example, an extortionist's letter sent to an intended victim could be examined by the law enforcement agency, but unless the extortionist consented, he could demand to be notified of his rights and could direct the destruction of evidence which would otherwise lead to his indictment. Likewise, persons who receive bomb threats, threatening telephone calls or ransom demands in a kidnapping case would be reluctant to give consent to the interception of a call, knowing that their cooperation with law enforcement authorities would be revealed upon demand.

Separate and apart from these considerations is the fact that Amendment (2) unjustifiably extends the Privacy Act to foreign nationals and to associations and corporations, both domestic and foreign. Presently, the Privacy Act extends protection to "a citizen of the United States or an alien lawfully admitted for permanent residence." The Department of Defense sees no justification for being required to disclose its investigative techniques to foreign

persons, such as a foreign intelligence agent. Counterintelligence operations of the Military Departments may well involve the collection of information through the interception of communications between witting and consenting sources of information and a known hostile intelligence agent. Existing practices with respect to authorized searches, mail covers, and the interception of communications with the consent of one party would virtually cease if there is a requirement that the hostile agent be notified of this practice. Even more unrealistic is the proposal that the investigating agency be required to destroy information about a hostile agent when he so directs. Consequently, broadening the scope of the Act to include other than United States citizens would seriously jeopardize our intelligence efforts and thereby cause irreparable damage.

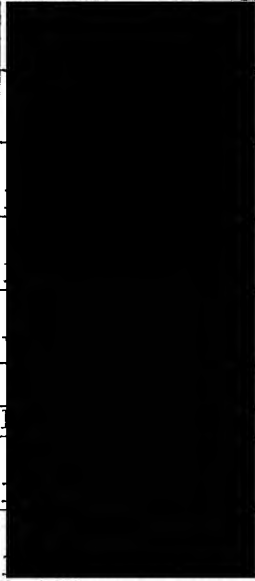
Finally, Amendment (2) raises a number of questions of interpretation. The wording of the proposed subsection 12A in Amendment (2) creates ambiguity as to which systems of records it applies. Is it meant to cover only those systems of records which are clearly delineated in the current Privacy Act, or all records of any nature which reflect the activities described in the Bill without regard to retrievability? The general tenor of the Bill strongly suggests that it is aimed at all files, however they may be constituted and whatever their nature. Amendment (2) is also drawn in such a way that it would apply to records created before the effective date of the Privacy Act of 1974. If this interpretation is correct,

historical files in the Government Archives, no matter how old, would have to be examined to determine whether any information contained therein is subject to the requirements of the Bill. A question also arises as to whether it is intended that documents pertaining to categories (A) and (B) must be destroyed by the Agency at the subjects insistence, whereas all other documents covered by the Privacy Act will be destroyed only if the Agency, in its exercise of administrative discretion, decides that it is in the public interest to do so.

However, because of its overbreadth, we cannot support the Bill in its present form. In summary, the Department of Defense has made a good faith effort to insure the proper balancing of interests in its implementation of the Privacy Act.


STATINTL

ACTION ROUTING SLIP

		
X		
G. Cary for signature		
SUSPENSE DATE: <u>Yesterday</u>		
RECEIVED IN OLC: <u>11 May 76</u>		

COMMENTS:

STATINTL

Called 
" May -
jdc